Very High-Performance Embedded Computing will allow Ambitious Space Science Investigation

Michel PIGNOL

CNES - Toulouse - France

michel.pignol@cnes.fr

RESUME : Jusqu'à présent, la définition des missions spatiales scientifiques était limitée par les composants électroniques autorisés par les Agences Spatiales, i.e. développées sur des technologies tolérantes aux radiations. Malheureusement, les microprocesseurs disponibles aujourd'hui sur de telles technologies ont la puissance de calcul qui était disponible il y environ 10 ans sur le marché commercial. Aujourd'hui, l'une des faiblesses principales des composants commerciaux dans le cadre d'une utilisation spatiale est leur sensibilité aux upsets, qui génèrent des fautes transitoires durant l'exécution des logiciels de vol. Aussi, à la condition d'avoir des architectures tolérantes aux fautes "légères", la communauté spatiale pourrait définir une nouvelle classe de missions scientifiques spatiales ayant des objectifs très ambitieux et en rupture avec les missions classiques grâce à la haute performance de calculateurs embarqués basés sur des composants électroniques commerciaux.

ABSTRACT : Up to now, the definition of space science missions was bounded by electronic components authorised by Space Agencies, i.e. developed on radiation tolerant technologies. Unfortunately, the microprocessors today available on such technologies have the computing throughput which was available about 10 years ago on the commercial market. Today, one of the main weakness of commercial components for space usage is their sensitivity to upsets, which generate transient faults during execution of flight software. Thus, to the condition to have "light" fault-tolerant architectures, the space community could define a new class of space science missions having very ambitious scientific goals and disrupting with classical missions thanks to high-performance embedded computers based on commercial electronic components.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
13 JUL 2005	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Very High-Performance Embedded Computing will allow Ambitious Space Science Investigation	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **CNES - Toulouse - France**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM001791, Potentially Disruptive Technologies and Their Impact in Space Programs Held in Marseille, France on 4-6 July 2005., The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**14**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

1 - INTRODUCTION

The computing power of commercial microprocessors largely exceeds one thousand MIPS (Mega Instructions Per Second) while their space counterparts reach a hundred or so. The almost fifty-fold ratio between these two families, favourable developments in semi-conductor technologies with respect to space constraints, and the new high computing power requirements of certain programs, make the possibility of using commercial microprocessors on board satellites more relevant than ever.

2 - THE HISTORY OF "COTS" STUDIES AT CNES

Studies about the use of Commercial Off-The-Shelf (COTS) electronic components for on-board applications were first begun by the CNES Product Assurance department around 1992.

For over 10 years, the CNES has been developing the expertise to allow the large scale usage of COTS on-board satellites, prompted by the decrease of the "space" components market and the improved reliability of commercial components. A intra-CNES multi-disciplinary working group was set up in mid-1995, and a "commercial components" project coordinated all studies on this subject between 2000 and 2002 [1]. A methodology for covering all the new aspects associated with COTS from a "Product Assurance" point of view was developed within the "Component multi-partnership" (*Multi-partenariat composants*) [2], a working group including: ALCATEL Space, EADS-ASTRIUM, EADS-ST, THALES, CNES.

Because "traditional" fault/failure-tolerant architectures seem very limiting (mass, volume, consumption, complexity, cost of development and validation, recurring cost), a study into the fault tolerance domain – required for using COTS – was initiated at CNES on this subject in mid-1995 with a view to seeking "lighter" architectures.

It should be noted that "low cost" scientific missions do not necessarily require a high level of availability. Commercial components can therefore be used in such cases without having to "pay" the extra price of fault-tolerant architectures (e.g., MYRIADE). However, in view of the increasing sensitivity of commercial components (finer lithography), it is not impossible that some of them may require protection against upsets.

3 - OVERVIEW OF DEVELOPMENTS IN "COTS" COMPUTERS

Commercial components are occasionally used for all types of functions. We are focussing here on the main component of computers, i.e. the microprocessor. The following is an overview of major projects or studies relating to the use of computers based on fault tolerance-protected commercial microprocessors in the space domain [3].

A solution called **EDDI** (Error Detection by Duplicated Instructions) developed by Stanford University, that has flown on the USAF Argos large satellite (launched on 1999), is based on time replication at instruction level [4]. The EDDI computer is based on the COTS IDT-3081 processor (R3000 instruction set). Over a 350-day period in orbit, 321 errors have been detected and 98,7 % have been corrected [5].

A solution called **TTMR** (Time Triple Modular Redundancy), that has been implemented into the Proton100k computer developed for space missions by SPACE MICRO is based on time replication at instruction level to [5]. It takes advantage of DSP (Digital Signal Processor) having VLIW (Very

Long Instruction Wide) parallelism for reducing the time processing overhead. The Proton100K will fly on the USAF Roadrunner experimental small satellite.

The **SCS750** space-qualified board has been developed by MAXWELL Technologies [6], based on three IBM PowerPC750FX microsynchronized microprocessors working in TMR (Triple Modular Redundancy, also called triplex) mode. The SCS750 will fly on the six-operational-satellite constellation NPOESS dedicated to civil/military weather forecasting (first launch planned in 2009).

The **REE** (Remote Exploration and Experimentation) program has been developed by JPL over a 10-year period [7]. JPL thus hopes to be able to use data processing computers for scientific payloads based on commercial components with semi-massively parallel architectures. Several fault-tolerant techniques, depending on the level of implementation (middleware, application level, etc.) and criticality of the tasks, was implemented; in particular, **ABFT** (Algorithm Based Fault Tolerance) techniques.

The Ariane 5 telemetry generation unit called **UCTM-C/D** developed by IN-SNEC, is a double-duplex based on DSP not immune to radiation.

The **GUARDS** architecture, based on the TMR technique, was developed within a major European project with three target applications: rail, nuclear and space systems (EADS-ASTRIUM, LAAS-CNRS, and other companies and laboratories) [8].

Following several studies [9], the **DMS-R** command-control computer for the Russian module on the ISS launched in 2000, consists of two triplex computers, both being based on a "three-chips ERC32" (EADS-ASTRIUM). A triplex system based on the DMS-R board and on Transputer microprocessors was developed for the ATV command-control computer called **FTC** (EADS-ST) [10]. The ATV also includes a **MSU** (Monitoring & Safing Unit), developed by SAAB Ericsson Space: two channels based on MA-31750 microprocessors running in duplex mode. These developments are based on radiation hardened components; nevertheless, the know-how resulting from these failure tolerant architectures could be applied for protecting COTS againts upsets.

The platform computer of the DLR **BIRD** micro-satellite launched in 2001 [11] is based on the PowerPC MPC623 micro-controller. It is built on a single board and there are four of these. Two channels are switched on and work in a duplex mode; the two other channels are switched off and used as spares in case of transient or permanent problems on the two other active channels. Over the first 20 months of orbital operation, upsets have been correctly passivated; only a single event required to switch the control of the satellite to the spare nodes.

The "studient" computer of the ISAS (Japan) **INDEX** micro-satellite (to be launched), is based on the Hitachi SH-3 commercial micro-controller protected by a "light" version of a triplex architecture (centralized voter) [12].

It should be noted on one hand the very small number of these developments which have flown, and on the other hand the diversity of fault tolerance solutions developed for the small space market (duplex, triplex, time replication, strutural replication, macro-synchronization, micro-synchronization, …).

4 - JUSTIFICATION OF THE USE OF "COTS" IN SPACE INDUSTRY

4.1 - GROWING INTEREST IN COTS IN THE SPACE DOMAIN

There were two main arguments that limited the use of commercial electronic components for space applications: the first of these was the availability of radiation-tolerant/hardened components, including microprocessors with adequate processing power for most needs (in other cases ASICs

and FPGAs were used); the other was the additional costs due to the fault-tolerant architectures required to protect the COTS (in particular the processors) from radiation-induced single event effects such as upsets (as well as the risks associated with using these new components and architectures).

However, recent facts in favour of commercial components make the possibility of using COTS on board satellites more relevant than ever:

- The very deep submicron semi-conductor technologies provide improved total dose and latch-up tolerance: the majority of COTS are now compatible with these space constraints;
- The emergence of commercial CMOS/SOI technologies that have reduced latch-up sensitivity (and even eliminated it completely in the case of "SOI Trench", the most usual technology), while at the same time reducing the power consumption at identical performance (the impact on total dose and upset tolerance may also be positive);
- The emergence of a market of very low consumption, very high performance components (PALM/PDA, portable PC, mobile telephone, automotive, etc.);
- The performance gap (in the general sense of the term) between space and commercial components that is steadily growing in accordance with Moore's law. In particular, the very high computing power provided by commercial microprocessors, leaves some free capacity for fault tolerance constraints (e.g. time replication), as well as allowing more numerous and/or more complex on-board functionalities to be envisaged than is possible with radiation-tolerant components.

All COTS used in space projects show that performance (in the broadest sense of the term: functionality, number of gates in FPGAs, operating frequency, computing power, power consumption, etc.) is the essential factor for their selection. Consequently, the analysis presented in this Section on the conditions for COTS to be used in the space industry on a larger scale than now, centres around the key computer component, the "microprocessor", and thus on the available computing power. In fact, the arrival of very high performance microprocessors in the space domain could considerably increase the potential number of on-board functions, thus allowing much more ambitious and innovative missions to be planned, totally different than those defined on the basis of traditional space components.

The facts relating to computing power are analysed in more detail below.

4.2 - COMPUTING POWER

4.2.1 - *A widening gap*

The computing power of COTS has greatly increased due to joint improvements in two areas:

- Technology: microprocessors very quickly incorporate the latest evolutions; most microprocessors are now produced using 0.13 µm process technology, IBM's PowerPC970FX even uses 90 nm technology.
- The architecture: the switch to so-called "superscalar" architectures has enabled American manufacturers to remain on course to maintain the rate of progress predicted by Moore's law.

Finally, COTS microprocessors achieve 7 GIPS [1] (IBM PowerPC970FX).

[1] All computing powers are quoted as "peak" rates.

The performance of COTS microprocessors is without equivalent in the space component sector as radiation-tolerant technologies, and the microprocessor architectures supported by these technologies, are lagging a few generations behind those of the COTS (typically 1 to 3 generations):

- In the USA: HONEYWELL with the RHPPC (0,35 µm, compatible with the MOTOROLA PowerPC603e [13]) and BAE Systems with the RAD750 (0,25 µm, compatible with the IBM PowerPC750 [14]) have radiation-hardened microprocessors of approximately 250 MIPS.
- In Europe: ATMEL manufactures the ERC32-SC in 0.35 µm providing 20 MIPS, which came out in 1998, as well as the LEON2 in 0.18 µm providing 80 MIPS dating from 2005. The architecture of the entire unit of the LEON2 is still based on that of the non superscalar SPARC manufactured by CYPRESS in 1987 (in 0.8 µm at the time) for which ESA acquired the licence.

Satellites that make large-scale use of commercial components are generally micro-satellites. These include, for example, MYRIADE, a family of micro-satellite platforms developed by CNES. Apart from these, COTS are only sporadicly used in satellites, and generally only where no space counterparts having equivalent performance exists. However, because of the exponential effect of Moore's law, the gap in computing power that exists between space and commercial technologies is continually growing (today reaching several GIPS!). Such a performance gap, in addition to facts referred to in Section 4.1, shows that the use of commercial microprocessors in satellites appears to be becoming unavoidable.

4.2.2 - *Alternative solutions to COTS*

Up until now, the usual solution in cases requiring a high level of computing power was to use DSP or ASIC.

The ATMEL TSC21020 signal processor has become obsolete. Its replacement is currently being analysed but is not yet certain.

The performance obtained thanks to the hardwired feature of radiation-tolerant ASICs is generally compensated by their lower clock speed than that of commercial microprocessors (as the technology is not of the same generation). The high cost of this solution also makes it unaffordable for small projects (cost of a 0.18 µm process foundry: approximately 600 k€, reduced to approximately 230 k€ in MPW "Multi-Projects Wafer"). Finally, this solution is not suitable for evolutionary functions (during development or in flight) that may be necessary in the scientific (adjustment of algorithms to face unanticipated events), or Telecom applications (see Section 4.4).

The "large FPGA" [2] technology that is currently emerging resolves certain of the weaknesses of ASIC (cost, reprogramming during development or even in flight), but the International Traffic in Arms Regulation (ITAR) rule that limits the distribution of these products (which are up to now from American sources) could reduce their range of use in the American market.

Commercial microprocessors are non-ITAR products (at least some of them) and provide maximum reprogramming flexibility. They are equally suitable for large and small budgets. Account must obviously be taken of the slowing of bus frequencies due to the external memory protection systems (partly compensated by large internal cache memories that are sometimes protected by integrated error-correction code), as well as of the additional cost due to protection against upsets being provided by a fault-tolerant architecture.

---

[2] In excess of one million gates.

ASICs and FPGAs do not therefore provide a universal solution to the need for computing power and can be complemented by up-to-date commercial microprocessors, the optimum solution depending on the needs of the project.

4.3 - HIGH COMPUTING POWER FOR SCIENTIFIC PAYLOADS

Scientific payloads are an area in which high computing power can be particularly attractive:

- In the field of scientific payloads, it is often the technology that gives rise to the mission. COTS make more ambitious missions feasible and could allow space science investigation to take a major step forward thanks to a level of on-board computing power that is vastly greater than that which has been used up until now.
- Some of the recent major European scientific satellite programmes (e.g., the ESA GAIA programme, the successor of HIPPARCOS) have shown a computing power requirement that cannot be achieved using radiation tolerant processors, while ASICs are unsuitable for this type of programme due to the need to adapt to changing scientific needs and processing algorithms throughout the programme, as well as the possibility of in-flight evolutions to adjust/adapt processing according to the initial results obtained in orbit.

In conclusion, it can be presumed that scientists have up until now (in particular for small missions) applied self-censorship when defining missions, in order to adjust the mission to the capabilities of radiation-resistant technologies (TSC21020, …). **The space industry now has a possibility to "change the scale" of space science investigation thanks to the on-board computing power available**. ASICs and FPGAs are a solution in some cases, but not all: flexibility of reprogramming (including in flight) and a non-ITAR classification remain the prerogative of microprocessors.

4.4 - HIGH COMPUTING POWER FOR REGENERATIVE TELECOM PAYLOADS

Let us take the example of the substantial payload of INMARSAT 4: certain unvarying functions are hardwired and performed using ASICs, but as the protocol and signalisation processing may potentially vary over time, they must be reprogrammable in flight. These functions are therefore performed using DSPs. In the end, the satellite carries several thousand ASICs and DSPs, the computer alone consumes 1,800 W in an enormous 150 kg case.

This example shows that there is a genuine need for high computing power and re-programmability where regenerative payloads are concerned. The use of commercial microprocessors (associated, if necessary, with a redundancy scheme allowing graceful degradation of performance) will represent an attractive solution when the satellite telecom operators (INTELSAT, EUTELSAT, SES Global, etc.) overcome their "psychological" resistance to the use of COTS.

4.5 - OTHER POTENTIAL COMPUTING POWER NEEDS

The advent of high computing power could be a significant advantage in certain areas:

- Flight software crisis:

  The on-board software has become increasingly critical in the development cycle of a satellite.

  Generally speaking, in software development, an increase in the level of abstraction using a methodology and/or a tool and/or a language will increase productivity while also ensuring greater software reliability, but this is achieved at the cost of on-board performance in terms of the volume of memory and execution time. The passage from coding in assembler to the use of a high level language is a very representative example.

The availability of high levels of computing power on-board satellites would therefore make it possible to envisage improving the software development cycle. This could be achieved by various techniques, all requiring larger execution times than usual methods:

- Software reuse (which will then increase in volume to take account of multiple contexts and operating conditions).
- Automatic code generation (the generated code is then de-optimised).
- Interpretation on board (greatly increases the flexibility of development and use of certain functions, but this technique is very costly from a computing power point of view).
- Use of freeware (not optimised for low computing power).
- Java language (improves portability but consumes an enormous amount of computing power).
- In-flight loading of new modules (technique used by NASA for the CASSINI-HUYGENS probe launched in 1997), which reduces the planning constraints on the development of certain non-vital parts of the software.

- Increased on-board autonomy:

  The increase in autonomy on board satellites is continuous.

  It is currently an area of very active research in which CNES and ONERA are cooperating. For example, long-range missions (Mars robots, interplanetary probes, etc.) require a high level of autonomy on board as the communication bandwidth is low.

  And on-board autonomy is intrinsically a consumer of computing power.

4.6 - FUNCTIONALITIES

Until recently, the space industry had often redeveloped its standards and its components, in particular in communication, in order to optimise protocols (security, etc.) and the electronic volume. For a few years now, however, space standards have tended to better model themselves on industrial standards (e.g., European standard ECSS-E-50).

The development of SoC (System on Chip) allowed the emergence of microcontrollers integrating increasing numbers of functions and multiple Input/Output interfaces. These SoCs are attractive and could allow to optimise the development of equipment (volume / consumption / development time) on condition that the main industrial communication standards are used in the satellites (bus I2C, bus CAN, etc.).

Furthermore, the availability of high levels of on-board computing power opens up a very wide range of new functionalities, such as those mentioned in Section 4.5.

5 - THE PROBLEM TO BE RESOLVED: FAULT TOLERANCE

It must be possible to "live" with upsets, as all commercial components are sensitive to them. Fault-tolerant architectures are therefore necessary to protect them. The protection techniques that can envisaged according to the type of function are presented in [15]. However, as "fault tolerance" is a new functionality, it represents an additional cost relative to usual computers. This overhead is due to the large effort required for studying/developing an optimal solution well-suited to the target application, and also to software mechanisms implementation, to hardware replication (recurring cost) and, last but not least, to validation during system integration. This latter parameter must not be minimized, as it requires costly fault-injection for system acceptance tests during the final

integration phase using specific tools with a "production" capability, not only for "laboratory demonstration".

Consequently, it is important to develop architectures that will minimise this additional cost. The CNES TAFT study (*Tolerance Aux Fautes Transitoires*, fault tolerance to transients) has allowed the development of two architectures that – in terms of complexity and performance – are situated somewhere between the following extreme solutions:

- A collection of basic detection mechanisms, e.g. global and local watchdogs with recovery contexts such as on MYRIADE. The error coverage rate of these basic mechanisms is low, but sufficient for certain missions (low specified mission availability requirement and/or use of relatively insensitive commercial components and/or low radiation constraints).
- The so-called "triplex" TMR architecture, with triple CPUs and majority voting on results. This architecture was envisaged for HERMES and used on the DMS-R of the ISS as well as on the ATV (see Section 3). The coverage rate is excellent, but this solution is costly.

The two CNES architectures include a time division duplex named DMT as well as a mini structural duplex named DT2.

The objective of the CNES, through this TAFT study, was to dispose of a "fault tolerance tool box", i.e. a series of validated solutions from which the fault-tolerant architecture best suited to the needs of each project could be chosen, the DMT and DT2 being two tools among several other ones in that box. Each architecture has advantages and drawbacks as shown in figure 1.

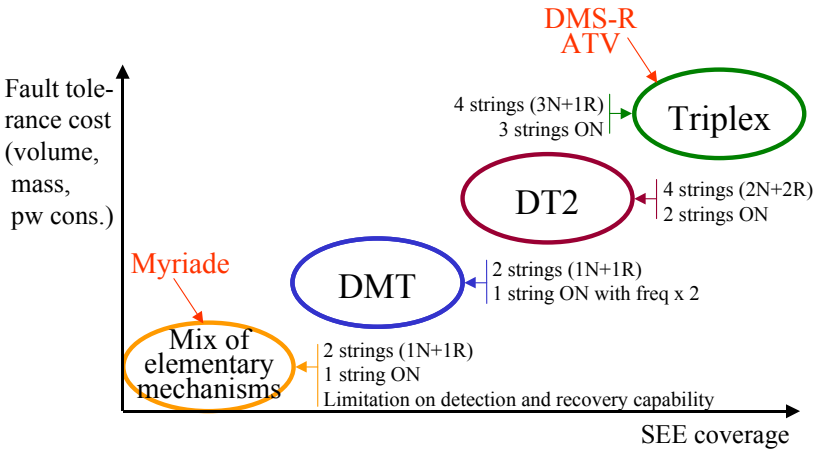

Figure 1 – Fault tolerance tool box

6 - TWO CNES "FT" ARCHITECTURES

Within the TAFT study, CNES targeted domains are from the low/medium processing performance range with possibly hard real-time and mission critical tasks (e.g., spacecraft control computers), to the high-end processing performance range (e.g., embedded processing for payload intelligent sensors) [16][17].

It was preferred to take advantage of the extra performance allowed by COTS with regard to needs for developing generic FT (Fault-Tolerant) architectures; they are well suited to a large range of

applications without requiring new development/validation phases when a given project selects one of them.

Two domains having specific features have been analyzed. Firstly, the scientific payloads and small satellites domain was targeted. The highest priority for these missions is to obtain a very low FT cost either in terms of weight or power consumption or development / recurring costs. On the other hand, the availability performance is not a strong constraint, and a large part of these applications accepts recovery of about 95 to 99 % of transient faults. This leads CNES to patent the DMT architecture.

Secondly, domain requiring a very high level of availability against transients (e.g. 99.9 %) was targeted, like control computers for large application satellites or data processing computers for applicative payloads (e.g., earth observation ones). For these missions, the FT extra costs are not as constraining as for the previous ones. This leads CNES to patent the DT2 architecture.

6.1 - DMT ARCHITECTURE OVERVIEW

DMT (***D**uplex **M**ultiplexé dans le **T**emps*, i.e. duplex in time) [18] is a low cost FT architecture based on time replication, and is macro-granularity oriented (based on operational task cycles): each operational task is executed twice successively (each execution being called VCi for "Virtual Channel number i"); during about one complete task iteration, the computer is working internally without check until it needs I/O (Input/Output) accesses.

Input must be centralized at the beginning of iterations, and output at their end (see figure 2). It means that each task iteration must be split in three distinct phases: data input "IN phase", then data processing "PRO phase", then data output "OUT phase".

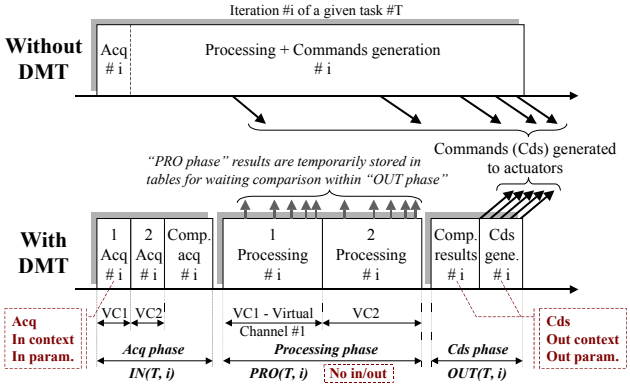

Figure 2 - DMT faults detection principle

Depending on the sensor type, the fault detection for the IN phase is based on time replication, then a threshold-based comparison allows to obtain acquisitions checking and consistency; when time replication is not possible, other usual methods are implemented.

The fault detection for the PRO phase is based on a bit-to-bit comparison (thanks to acquisitions consistency) at the beginning of OUT phase. Only the main results are compared: commands to actuators, parameters to other tasks, current context. All variables which are local to the task are not checked, thus reducing to few items the data to be compared.

A duplex is mainly a fail-stop architecture: it is able to detect faults, not to recover them because it can not intrinsically identify which of the channels is faulty. Thus, DMT architecture implements

specific mechanisms for having recovery capability, based on a safe context storage independent for each virtual channel:

- safe with regard to direct SEE: the external memory is considered as SEE-free because it is EDAC (Error Detection And Correction) protected;
- and safe with regard to faulty microprocessor accesses: the only needed hardware support mechanism is a "memory and I/O access checking" function, called CESAM, which is working like a MMU (Memory Management Unit) but including DMT specific mechanisms; it has to be implemented inside a FPGA or an ASIC designed to be SEE-free.

Within DMT, two recovery modes are implemented (see figure 3). Payload computers will mainly require *forward recovery*. Control computer will probably need *backward recovery* for few tasks; then a mix of these two recovery modes will be well suited.

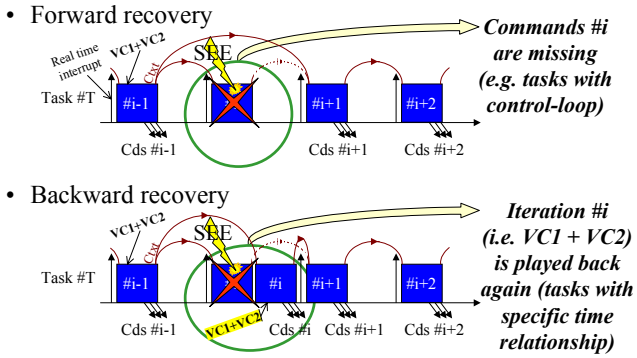

Figure 3 - Two DMT recovery modes

The DMT is compatible with preemptive scheduling.

For missions having not strong availability constraints, nothing could be done to protect the execution of the Real Time Kernel (RTK), a fault during RTK code execution being not detectable. For increasing availability performances of either the DMT or the DT2 architectures, a protection of the RTK code has been developed by CNES for "white/grey box" RTK (i.e. the source code of the RTK must be available because few modifications of this code are required).

6.2 - DT2 ARCHITECTURE OVERVIEW

DT2 (**D**ual **D**uplex **T**olerant to **T**ransients) [19] is a low cost and high performant FT architecture based on a mini-duplex structure:

- The duplication is limited to the PUC (Processing Unit Core), i.e. the microprocessor, its companion chip and its memory.
- Eeach PUC runs asynchronously the same flight software.
- The PUC macrosynchronisation is made only on external I/O data flow (i.e. sensors and actuators data). It should be noticed that a microsynchronisation version of the DT2 has been studied, but the macrosynchronisation one is only presented.
- The DT2 granularity is the same than the DMT one.

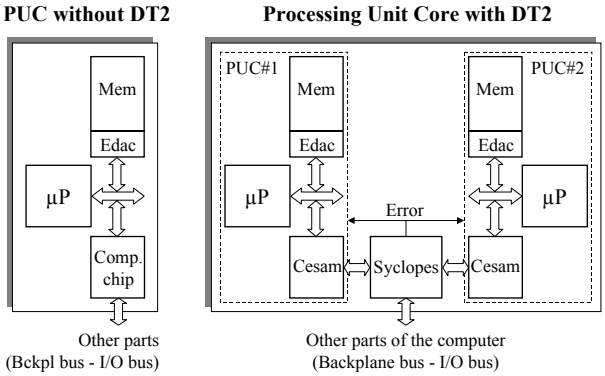

Figure 4 - DT2 hardware architecture

Only the heart of the nominal computer architecture is presented in figure 3, a redundant computer (in cold redundancy) being generally present in the space domain.

Two specific hardware functions are required, which have to be implemented inside an SEE-free FPGA or ASIC:

- CESAM, a simplified version of the CESAM used for the DMT,
- SYCLOPES which is in charge of three functions: macrosynchronisation, comparison, intelligent I/O coupler.

The recovery strategies are the same than the DMT ones: the recovery is also based on a safe context storage independent for each virtual channel thanks to CESAM and EDAC. Any PUC is knowing if the other is healthy or faulty; when SYCLOPES detects an error, then each PUC either simultaneously roll-back the faulty iteration within *backward recovery* mode or simultaneously cancel the faulty iteration and go to the next one within *forward recovery* mode; this is made without data exchange between both PUC thanks to the fact that each PUC has its own safe context storage inside its own memory.

The DT2 is compatible with preemptive scheduling.

Due to the fact that a high level of detection/recovery performance is reached for the DT2, only a complete and efficient protection of the RTK must be considered. As already mentionned, such protections of the RTK code have been developed by CNES.

6.3 - VALIDATION METHODOLOGY

The methodology used for the DMT/DT2 validation is based on two phases [20]: deterministic injection (software injection which is reproducible, thus "debug" oriented) and random injection (heavy ions injection, thus "extensive injection" and "global validation" oriented). These two phases have specific and complementary features in order to have a solid validation file to convince project teams.

7 - HIGH-PERFORMANCE EDAC

An important feature about the high performance of embedded computers lies in the memory bandwidth which must be often limited due to the use of EDAC (Error Detection And Correction) components.

Memory protections against upsets are widely implemented by the computer community. In the space domain, EDAC components have been implemented since a long time. But deep-submicron technologies bring more sensitivity to memory chips, and the EDAC propagation delay becomes more and more constraining as processors speed increase. A new architectural concept has been developed and patented by CNES for trying to reach the "zero delay penalty EDAC" [21][22][23].

It is based on concepts like: high pipeline stage number, error detection done in parallel with the data propagation into the pipeline of the processor, codage calculation done in parallel with data storage into memory, "associative memory" architecture. This EDAC architecture is compatible with every code (Hamming, Reed-Solomon, etc.), so it is very well suited for complex codes requiring long calculation delays. Such an EDAC is fully applicable for all "in house" developments integrated into ASIC/FPGA (e.g., custom processors for data processing as either FFT or data compression) and also commercial processors/IP (Intellectual Property) having means to interrupt the propagation of a data into their internal pipeline stages.

8 - CONCLUSION

The arguments have been presented in favour of using commercial microprocessors, protected by a fault-tolerant architecture where the needs of the mission require such protections. This solution is in addition to radiation-tolerant or hardened microprocessors and to ASIC/FPGA solutions, all of them being complementary.

It seems unavoidable that the space industry must one day have recourse (at least for specific needs) to components providing a very high level of on-board computing power together with reprogramming flexibility (including in flight). To begin with, the first applications in which commercial microprocessors would provide an undeniable advantage could be in the domain of scientific payloads and data processing computers.

In order to be able to "live with" upsets, the CNES has developed DMT and DT2, two fault-tolerant architectures that are well suited to space application constraints. The objective of the CNES being to be able to propose the most suitable solution for a given project, it has developed a "fault tolerance tool box", which includes the DMT and DT2 architectures as well as other solutions adapted to the use of COTS in space applications (purely software solutions, TMR, etc.).

The possibility of using microprocessors with a very high computing power on-board satellites should, in particular, allow more ambitious scientific missions to be planned than those currently defined for space microprocessors and, consequently, a major step forward in space science investigation could be done. The reduction in the cost of the flight software and the increase in its reliability could also result from the availability of high on-board computing performance. On-board autonomy would also be improved.

Thus, commercial components, and particularly microprocessors, pertain to the technologies having a potential disruptive capability for space missions.

9 - BIBLIOGRAPHY

[1] C. Aicardi, P. Lay, A. Mouton, C. Revellat, D. Beauvallet, G. Lemarchand and al., "Guidelines for commercial parts management", *European Space Components Conf. (ESCCON)*, 2002.

[2] COTS methodology, see documents reference RNC-Q-60-XX within the *Référentiel Normatif du CNES* (CNES normative documents database).

[3] M. Pignol, "How to Cope with SEU/SET at System Level?", *IEEE Int. On-Line Testing Symp. (IOLTS)*, 2005.

[4] M.N. Lovelette, P.P. Shirvani., E.J. McCluskey, et al., "Strategies for Fault-Tolerant, Space-Based Computing: Lessons Learned from the ARGOS Testbed", *IEEE Proc. of Aerospace Conf.*, vol. 5, pp. 2109-2119, 2002.

[5] D. Czajkowski, and M. McCartha, "Ultra Low-Power Space Computer Leveraging Embedded SEU Mitigation", *IEEE Proc. of Aerospace Conf.*, vol. 5, pp. 2315-2328, 2003; http://www.spacemicro.com.

[6] R. Hillmand, G. Swift, et al., "Space Processor Radiation Mitigation and Validation Techniques for an 1800 MIPS Processor Board", *Nuclear and Space Radiation Effects Conf. (NSREC)*, 2003; http://www.maxwell.com/go/scs750a.html.

[7] K. Whisnant, R. Some, D.A. Rennels, et al., "An Experimental Evaluation of the REE SIFT Environment for Spaceborne Applications", *IEEE/IFIP Proc. on Dependable Systems and Networks Int. Conf. (DSN)*, 2002; http://ree.jpl.nasa.gov/.

[8] D. Powell (Ed.), "A Generic Fault-Tolerant Architecture for Real-Time Dependable Systems", *Kluwer Academic Publishers*, ISBN 0-7923-7295-6, 2001.

[9] C. Guidal, and P. David, "Development of a Fault Tolerant Computer System for the HERMES Space Shuttle", *IEEE Proceedings on Fault-Tolerant Computing Symposium (FTCS-23)*, 1993.

[10] G. Urban, H-J. Kolinowitz, and J. Peleska, "A Survivable Avionics System for Space Applications", *IEEE Proceedings on Fault-Tolerant Computing Symposium (FTCS-28)*, pp. 372-381, 1998.

[11] P. Behr, W. Bärwald, K. Briess, and S. Montenegro, "Fault Tolerance and COTS: Next Generation of High Performance Satellite Computers", *DAta Systems In Aerospace Conference (DASIA)*, session 14A, 2003.

[12] H. Saito, M. Hirahara, S. Okano, et al., "INDEX: Piggy-Back Satellite for Aurora Observation and Technology Demonstration", *51th IAF International Astronautical Congress*, 2000.

[13] G.R. Brown, "Radiation Hardened PowerPC603e based single board computer", *IEEE Proc. of Digital Avionics Systems*, vol. 2, pp. 8.C.1.1-8.C.1.12, 2001; http://content.honeywell.com/dses/products/data/rad/default.htm.

[14] R.W. Berger, et al., "The RAD750 - A Radiation Hardened PowerPC Processor for High Performance Spaceborne Applications", *IEEE Proc. of Aerospace Conf.*, vol. 5, pp. 2263-2272, 2001; http://www.iews.na.baesystems.com/ads/.

[15] M. Pignol, et al., "Radiation Effects on Digital Systems", *Space Technology Course - Space Radiation Environment and its Effects on Spacecraft Components and Systems (SREC04)*, Section III-03, pp. 411-459, Cépaduès Editions, ISBN 2-85428-654-5, 2004.

[16] M. Pignol, "CNES Fault Tolerant Architectures Intended for Electronic COTS Components in Space Applications", *Proc. European Commercialisation of Military and Space Electronics Conf. (CMSE-6)*, pp. 39-48, 2002.

[17] M. Pignol, "DMT and DT2: Overview of two CNES Fault-Tolerant Architectures Intended for Electronic COTS Components in Space Applications", *IEEE Proc. Dependable System and Network (DSN)*, Supplemental Volume – Fast Abstract, pp. B34-B35, 2003.

[18] M. Pignol, "Method for processing an electronic system subjected to transient error constraints", European patent EP 1 121 642 B1.

[19] M. Pignol, "Computer system that tolerates transient errors and method for management in a system of that type", European patent EP 1 240 587 B1.

[20] M. Pignol, "Overview of the Methodology and Tools Developed for the Validation of CNES Fault-Tolerant Architectures", *IEEE Proc. Dependable System and Network (DSN),* Supplemental Volume – Fast Abstract, pp. 144-145, 2004.

[21] M. Pignol, "Device and method for detecting and correcting memory errors in an electronic system", European patent EP 1 340 148 B1.

[22] M. Pignol, "Coding device and method for a storage error detection and correction assembly in an electronic system", European patent EP 1 340 147 B1.

[23] M. Pignol, "Overview of a New CNES Architectural EDAC Concept for High Speed Memory Protection", *IEEE Proc. Dependable System and Network (DSN)*, Supplemental Volume – Fast Abstract, 2005.